

CLAIMS

We claim:

1. An apparatus for operating in a block-oriented safety related open control system comprising:
 - a memory, which includes at least one safety related component;
 - a processor, operably connected to the memory, wherein the processor executes the safety related component based on a system schedule; and
 - a medium attachment unit, which translates input messages and output messages between the processor and a transmission medium using an extended safety-related protocol.
2. The apparatus of claim 1, wherein the safety related component further comprises a function block which includes at least one device description.
3. The apparatus of claim 1, wherein the memory includes a plurality of safety-related function blocks and wherein at least one of the safety-related function blocks receives analog input data and makes the analog input data readable to another one of the plurality of safety-related function blocks as an output.
4. The apparatus of claim 3, wherein the plurality of function blocks include at least one SISFB.
5. The apparatus of claim 1, wherein the memory includes a plurality of function blocks and wherein at least one of the plurality of function blocks receives discrete input data and makes the discrete input data electronically readable to another one of the plurality of function blocks as an output.
6. The apparatus of claim 5, wherein the plurality of function blocks include at least one safety-related function block.
7. The apparatus of claim 1, wherein the memory stores a plurality of function blocks, including a non-safety-related function block and a safety-related function block, and wherein a non-safety-related function block and a safety-related function block are interconnected to communicate data only from the safety-related function block to the non-safety-related function block.

8. The apparatus of claim 7 wherein the processor controls the execution of the plurality of function blocks according to the system schedule.
9. The apparatus of claim 1, wherein the apparatus is operably connected to a digital bus.
10. The apparatus of claim 1, wherein the safety-related function block has an input and output and the memory further includes:
 - a safety-related resource block;
 - a first safety-related transducer block; and
 - a second safety-related transducer block;wherein the resource block insulates the safety-related function block from physical hardware, the first safety-related transducer block decouples the input to the safety-related function block, and the second safety-related transducer decouples the output of the safety-related function block.
11. The apparatus of claim 1, wherein the memory further stores at least one object selected from the group consisting of: function blocks, flexible function blocks, safety-related function blocks, safety-related flexible function blocks, safety-related transducer blocks, safety-related resource blocks, safety-related link objects, trend objects, alert objects, and view objects.
12. The apparatus of claim 11, wherein a resource is defined by the plurality of function blocks and at least one object.
13. The apparatus of claim 1, wherein the extended safety-related protocol includes an authenticator utilized to authenticate a message communicated between two safety related function blocks meets certain safety requirements.
14. The apparatus of claim 13, wherein the authenticator is CRC-32 compliant.
15. The apparatus of claim 13, wherein the authenticator is generated based upon data contained in the input message, a sequence number, a connection key and an object index.
16. The apparatus of claim 13, wherein the extended safety-related protocol utilizes a sequence number to generate the authenticator.

17. The apparatus of claim 13, wherein the extended safety-related protocol provides for the generation of a virtual protocol data unit prior to communication of a message to a safety related function block.
18. The apparatus of claim 1, wherein the transmission medium further comprises a black channel.
19. The apparatus of claim 18, wherein communications over the black channel between safety-related function blocks includes the transmission of an authenticator.
20. The apparatus of claim 1, wherein communications over the transmission medium are monitored for timely delivery.
21. The apparatus of claim 20, wherein the apparatus further comprises a watchdog timer configured to monitor whether an output safety-related function block is timely executed.
22. The apparatus of claim 1, wherein the memory further includes a diagnostic transducer block.
23. The apparatus of claim 22, wherein the diagnostic transducer block monitors the transmission medium for errors which may occur in the communication of messages between safety-related function blocks.
24. The apparatus of claim 23, wherein the errors monitored by the diagnostic transducer blocks includes timing errors, sequence errors, authentication errors masquerading errors, queuing errors and insertion errors.
25. The apparatus of claim 1, wherein the memory further comprises a write lock; wherein the write lock prohibits writing data into a safety-related function block when a resource associated with the safety-related function block is in other than an out of service mode or a manual mode.
26. The apparatus of claim 1, wherein the memory further comprises a module configured to detect communication delays between a publisher and a subscriber.

27. The apparatus of claim 26, wherein the module detects queuing in the black channel.
28. The apparatus of claim 26, wherein the module detects queuing errors based upon a comparison of a communicated sequence number and an expected sequence number.
29. The apparatus of claim 28, wherein the expected sequence number is computed independently by a receiver of the communicated sequence number.
30. A system for permitting interoperability between safety and non-safety related devices in a block-oriented open control system comprising:
 - a plurality of safety and non-safety related devices, at least one safety related device including an safety-related resource block and an safety-related function block; wherein the safety-related resource block uniquely identifies a safety-related resource provided in the safety related device and the safety-related function block processes parameters associated with the safety-related resource to produce an output message; and
 - a medium attachment unit, operably connected to at least the safety-related function block, wherein the medium attachment unit translates an input message from a transmission medium to the safety-related function block and the output message from the safety-related function block to the transmission medium using an extended safety-related protocol.
31. The system of claim 30, wherein each device includes a memory containing a system schedule, and wherein each safety-related function block is executed according to the system schedule.
32. The system of claim 30, wherein at least one device includes at least one safety-related function block and at least one standard function block.
33. An apparatus for enhancing interoperability of a block-oriented open control system with safety related devices, the apparatus comprising:
 - means for storing at least one safety-related function block, which includes contained parameters and a computer program, wherein the safety-related

function block includes end-user configured parameters and an end-user configured algorithm;

means, coupled to the storing means, for processing the safety-related function block using the contained parameters, wherein the processing of the contained parameters produces an output parameter; and

means, coupled to the processing means, for translating messages from the processor for transmission on a transmission medium using an extended safety-related protocol.

34. The apparatus of claim 33, wherein the storing means stores a system schedule and a plurality of function blocks, standard and flexible, and the processing means controls the execution of the plurality of function blocks according to the system schedule.
35. The apparatus of claim 33, wherein the storing means also stores a system schedule and the processing means processes the encapsulated safety-related function block according to the system schedule.
36. An apparatus operating in a block-oriented open control system which includes safety related components, the apparatus comprising:
 - a user layer, which includes an safety-related function block to provide functionality, wherein the safety-related function block includes end-user configured parameters and an end-user configured algorithm;
 - a physical layer, which translates messages from a transmission medium into a suitable format for the user layer and from the user layer into a signal for transmission on the transmission medium using an extended safety-related protocol; and
 - a communication stack, connected to the user layer and the physical layer, wherein the communication stack includes a data link layer and an application layer, wherein the data link layer controls the transmission of messages onto the transmission medium and the application layer allows the user layer to communicate over the transmission medium.
37. The apparatus of claim 36, wherein the user layer includes a plurality of blocks interconnected to perform a desired function.
38. The apparatus of claim 37, wherein the plurality of blocks includes a safety-related resource block, a safety-related function block and a safety-related transducer block.
39. The apparatus of claim 37, wherein the plurality of blocks includes at least one standard function block and at least one safety-related function block.
40. The apparatus of claim 39, wherein standard function block and a safety-related function block are distributed over a plurality of devices.

41. A memory for storing data for access by an application framework operating in a device within a block-oriented open control system with safety related components, the memory comprising:

- a data structure stored in the memory, the data structure including:
 - a safety-related function block;
 - a safety-related resource block, which makes hardware specific characteristics of the device electronically readable; and
 - at least one safety-related transducer block, wherein the at least one transducer block controls access to the safety-related function block.

42. The memory of claim 41, wherein the data structure also includes a directory object to store a list of references to the safety-related resource block, function block and transducer block.

43. A process for communicating safety related data from a publisher to a subscriber over an open control system, comprising:

- obtaining information useful in generating a first data sequence;
- generating the first data sequence using the obtained information;
- generating a first authenticator for the first data sequence;
- generating a second data sequence, wherein the second data sequence includes the safety related data and the first authenticator;
- communicating the second data sequence from the publisher to the subscriber;
- receiving a second prime data sequence which includes a received authenticator and received data; wherein the content of the second prime data sequence may vary from the content of the second data sequence;
- generating a third data sequence at the subscriber using at least one sequence of data obtained from the second prime data sequence;
- calculating a second authenticator at the subscriber based upon the third data sequence;
- comparing the second authenticator to the received authenticator;
- rejecting the second prime data sequence from further processing when the received authenticator and the second authenticator are different; and

accepting the second prime data sequence when the received authenticator and the second authenticator are the same.

44. The process of claim 43, wherein the open control system further comprises a fieldbus Architecture.
45. The process of claim 43, wherein the information useful in generating the first data sequence further comprises message data, a sequence number, an object index and a connection key.
46. The process of claim 45, wherein the connection key is obtained from a virtual communications relationship specified between the publisher and the subscriber.
47. The process of claim 43, wherein the first data sequence further comprises a virtual protocol data unit.
48. The process of claim 47, wherein the virtual protocol data unit further comprises a sequence of bytes including, in order, a connection key, a sequence number, an object index and data, the data including an object value and status.
49. The process of claim 48, wherein the connection key further comprises a unique number identifying a publisher-subscriber virtual communications relationship.
50. The process of claim 43, wherein the first authenticator is generated using a cyclic redundancy check.
51. The process of claim 43, wherein the first authenticator and second authenticators are generated using at least a thirty-two bit cyclic redundancy check.
52. The process of claim 43, wherein the second data sequence further comprises an actual protocol data unit.
53. The process of claim 52, wherein the second data sequence is communicated over a black channel, wherein the black channel further comprises a fieldbus Architecture.

54. The process of claim 43, wherein the third data sequence further comprises an expected protocol data unit, the expected protocol data unit further comprising a sequence of bytes including, in order, an expected connection key, a received sequence number, an expected object index and received data, the received data including an object value and status; wherein the received sequence number and received data are obtained from the second prime data sequence.
55. The process of claim 43, further comprising:
 - obtaining from the second prime data sequence a received sequence number;
 - obtaining an expected sequence number;
 - comparing the received sequence number to the expected sequence number;
 - if the sequence numbers are the same: accepting the second prime data sequence for further processing; and
 - if the sequence number are not the same:
 - rejecting the second prime data sequence.
56. The process of claim 43, further comprising implementing a watchdog timer, whereupon receiving the second prime data sequence after the expiration of the watchdog timer, the subscriber rejects the second prime data sequence.